Juha Kirsi

Avoimen lähdekoodin virtuaalipalvelinympäristö jälleenmyyntitarkoituksiin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

8.5.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Juha Kirsi Avoimen lähdekoodin virtuaalipalvelinympäristö jälleenmyyntitarkoitukseen. 30 sivua 8.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	yliopettaja Matti Puska

Työn tarkoituksena oli suunnitella ja toteuttaa palvelinalusta, johon voidaan luoda asiakaskohtaisia verkkoja sekä palvelimia. Työn tilaajana toimi yksityisyrittäjä, jolla oli tarve päästä käsiksi käyttäjätunnuksiin ja salasanoihin turvallisesti useasta toimipisteestä.

Työssä toteutettiin virtuaalipalvelinalusta avoimen lähdekoodin järjestelmällä. Tälle alustalle saatiin asennettua Windows ja Linux käyttöjärjestelmillä varustettuja virtuaalikoneita. Koneille asennettiin erinäisiä palveluita tukemaan asiakkaan toimintaa tai omaa ympäristöä. Oman ympäristön valvontaa varten asennettiin esimerkiksi tunnettujen laitteiden liikennemääristä ja kuormituksesta kuvaajia piirtävä palvelin. Kriittisiä laitteita valvova ja uusista verkkoon liitetyistä laitteista hälyttävä palvelin. Asiakkaalle asennettiin sisäverkon palveluja tuottava palvelin, jonne asennettiin selaimessa toimiva salattu salasanatietokanta.

Koneiden verkkoliikenne kyettiin eristämään toisistaan käyttämällä VLAN-tekniikkaa. Oletusyhdyskäytävän kautta tapahtuvaa reititettyä liikennettä rajoitettiin palomuurisäännöillä. Pääsy yksityisiin asiakasverkkoihin sallittiin asiakkaan VPN-tunneliverkosta. VPN yhteydet toteutettiin käyttäen OpenVPN protokollaa.

Asiakkaan kokemukset ja palaute palvelun käytöstä olivat positiivisia.

Avainsanat	virtuaalialusta, Xen, pfSense, VPN, VLAN

Author	Juha Kirsi
Title	Open source virtual environment for resale purposes
Number of Pages	30 pages
Date	8 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Matti Puska, Principal Lecturer

The purpose of the project described in this thesis was to design and implement a server platform that could be customized to create client specific networks and servers. The client who ordered this thesis is an entrepreneur with the need to access his customer case credentials from multiple sites with ease and a secure connection.

First, an open source virtualization platform was installed onto the servers, and virtualized Windows and Linux machines were installed on the platform. The machines hosted several applications to support customer cases and the server environment itself. In addition, a network metric collection server and a network scanner server with alarm capabilities were implemented for server monitoring purposes. For the client a server hosting web pages for intranet was equipped with a username and password database web application.

Traffic between networks was isolated with the VLAN technique. Traffic routed through the default gateway was restricted with firewall rules. Access to individual client networks was granted through specified VPN networks. The VPN connections were implemented using the OpenVPN protocol.

In conclusion, customer experiences and feedback from the use of the service were positive.

Keywords	Virtualization, Xen, pfSense, VPN, VLAN

Sisällys

Lyhenteet

AD	*Active Directory*. Windows-palvelinympäristön aktiivihakemisto käyttäjien hallintaan.
AH	*Authentication Header.* Tarjoaa todennuksen ja takaa viestien eheyden IPsec liikenteessä.
BSD	*Berkeley Software Distribution*. Nimitys toiselle Unix-päähaaralle ja siitä polveutuville järjestelmille.
BIND	*Berkeley Internet Name Domain.* Nimitys nimipalvelinohjelmistolle.
CD	*Compact Disc*. Optinen tallennusmedia.
CIFS	*Common Internet File System*. Tiedostojen jakoon käytettävä verkkoprotokolla Windows ympäristöissä.
DMZ	*Demilitarized Zone*. Fyysinen tai looginen aliverkko organisaation oman verkon ja julkisen verkon välissä.
DNS	*Domain Name System.* Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
DVD	*Digital Video Disc.* Optinen tallennusmedia.
ESP	*Encapsulating Security Payload.* IPsec pakettivirtojen turvaamiseen käytetty protokolla.
GB	*Gigabyte.* Tietotekniikassa käytettävä mittayksikkö tallennuskapasiteetille.
GPL	GNU *General Public License.* Vapaiden ohjelmistojen julkaisemiseen tarkoitettu lisenssi.
IETF	*The Internet Engineering Task Force.* Internet-protokollien standardoinnista vastaava organisaatio.

IP	*Internet Protocol.* TCP/IP mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä verkossa.
IPAM	*IP Address management.* IP-aliverkkojen hallintaan ja dokumentointiin käytettävä työkalu.
IPSEC	*IP Security Architecture.* Joukko tietoliikenneprotokollia Internet yhteyksien turvaamiseen.
iSCSI	*Internet Small Computer System Interface.* Standardi tiedon välittämiseksi tietokoneen ja tallennuslaitteen välillä IP-verkossa.
KVM	*Kernel -based Virtual Machine.* Täysi virtualisointiratkaisu Linuxille.
L2TP	*Layer 2 Tunneling Protocol.* VPN-tunnelointiprotokola.
LACP	*Link Aggregation Control Protocol.* Protokolla usean fyysisen tiedonsiirtoportin yhdistämiseksi yhdeksi loogiseksi portiksi.
LAN	*Local Area Network.* Rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko.
NAS	*Network Attached Storage.* Tiedostojen jakamiseen tarkoitettu verkkolaite.
NFS	*Network File System.* Tiedostojenjakoon käytettävä verkkoprotokolla UNIX-johdannaisissa ympäristöissä.
NVRAM	*Non-Volatile Random-Access Memory.* Muistipiirityyppi, joka säilyttää sisältämänsä informaation myös virrattomana.
OSI	*Open Systems Interconnection model.* Kuvaus tiedonsiirtoprotokollien yhdistelmän seitsemästä kerroksesta.
PPTP	*Point to Point Tunneling Protocol.* VPN-tunnelointiprotokolla, jonka käyttö on pääosin lopetettu L2TP:n korvaamana.

RADIUS *Remote Authentication Dial In User Service.* Protokolla verkon käyttäjien tunnistukseen, valtuutukseen ja tilastointiin.

RAID *Redundant Array of Independent Disks*. Tekniikka, jolla tietokoneiden vikasietoisuutta ja/tai nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi.

RFC *Request for Comments.* IETF-organisaation julkaisemia Internetiä koskevia standardeja.

SAN *Storage Area Network.* Levyjärjestelmien verkko, jolta palvelimet saavat lohkotasolla levytilaa, esimerkiksi iSCSI protokollaa hyödyntäen.

SNMP *Simple Network Management Protocol*. Verkonvalvontaprotokolla, jolla voidaan valvoa ja hallita verkkolaitteita jotka tukevat tätä protokollaa.

SSL *Secure Sockets Layer.* Sertifikaatteihin perustuva tiedonsiirron salausprotokolla.

TCP *Transmission Control Protocol.* Internet-liikenteen ydinprotokolla, joka tarjoaa luotettavan, järjestyksellisen ja virhetarkistetun tiedonsiirron.

TLS *Transport Layer Security.* Sertifikaatteihin perustuva tiedonsiirron salausprotokolla.

UDP *User Datagram Protocol.* Yhteydetön tiedonsiirtoprotokolla.

VM *Virtual Machine.* Virtuaalikone.

VPN *Virtual Private Network.* Virtuaalinen erillisverkko.

WWW *World Wide Web.* Internet-verkossa toimiva hajautettu hypertekstijärjestelmä

XAPI *Xen Management Application Programming Interface.* Rajapinta Xen käyttöjärjestelmän työkalujen hallintaan.

XCP *Xen Cloud Platform.* Avoimen lähdekoodin virtualisointialusta.

ZFS *Zettabyte File System.* Solarista varten kehitetty tiedostojärjestelmä, nykyisin käytössä mm. FreeBSD:ssä ja johdannaisissa.

1 Johdanto

1.1 Historiaa

Perinteinen lähestymistapa uuden sisäverkon palvelun tuottamiseksi yritykseen on ollut kallis hankinta- ja ylläpitokustannuksiltaan. Jokaista erillistä palvelua varten on hankittu oma fyysinen palvelinlaite ja tarvittavat ohjelmistot. On tarvittu investointeja oman infrastruktuurin kehittämiseen sekä täytynyt palkata osaajia sen ylläpitämiseen.

Hankintapäätöksestä valmistumiseen on kulunut huomattavan paljon aikaa, johtuen laitteen tilaukseen liittyvistä prosesseista. Ensin kone täytyy saada lähtemään toimittajalta ja kuljettaa asiakkaalle. Tämän jälkeen jonkun on täytynyt asentaa laite laitetilaan, asentaa käyttöjärjestelmä, tarvittavat ajurit ja päivitykset. Viimeisenä on vasta itse sovelluksen asentaminen ja määrittely. Vaiheita on siis useita ja niiden välissä on usein myös odottelua, että tehtävään sopiva henkilöresurssi saadaan paikalle tekemään kyseinen toimenpide. Tähän kaikkeen on saattanut kulua päiviä, jollei jopa viikkoja.

Vikatilanteissa palvelukatkot ovat vaikeita välttää, sillä komponenttien vaihdon ajaksi palvelin tulee sammuttaa. Palvelinlaitteelle asennettuja sovelluksia ei voida sinä aikana käyttää [11, s. 4 – 5.]

1.2 Työn lähtökohdat

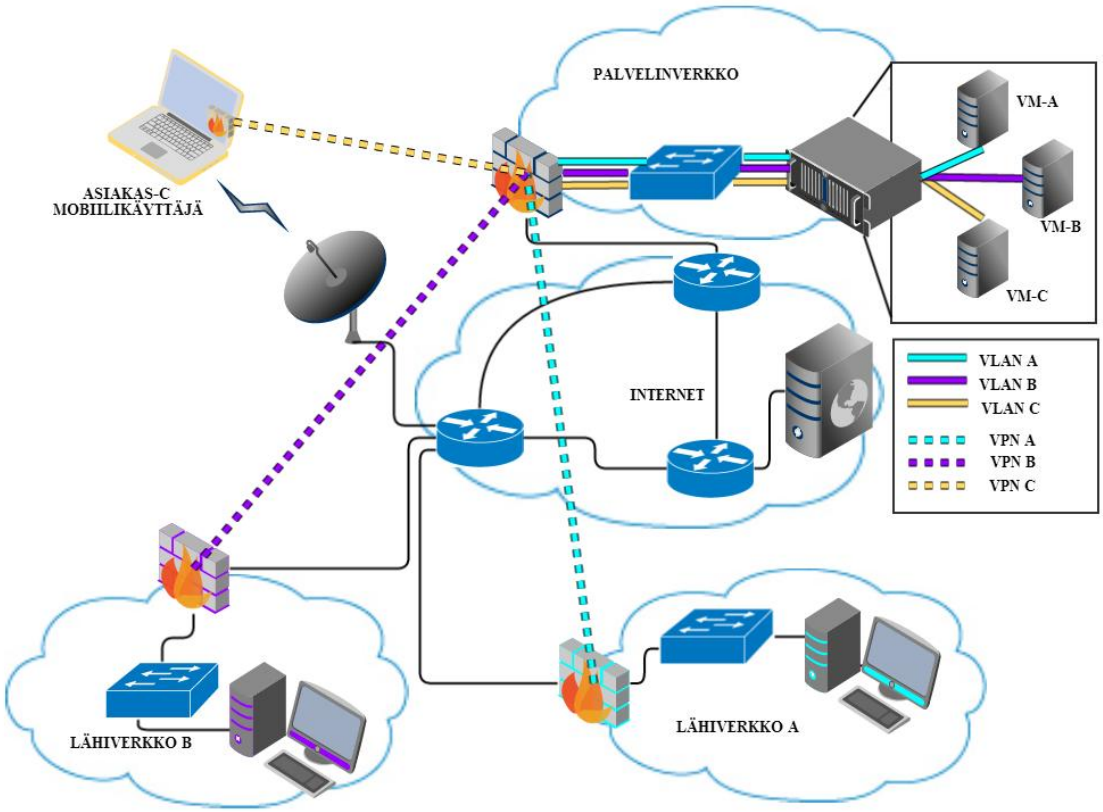
Tämän työn lähtökohtana on rakentaa omaan käyttöön moniasiakasympäristöön soveltuva palvelinympäristö. Työn tilaajana toimii Tmi M Design, joka suunnittelee ja tuottaa www-sivuja sekä painotuotteita. Tmi M Design tarvitsi ratkaisua asiakastunnusten hallintaan. Toteutuksen piti olla helppokäyttöinen, turvallinen sekä tavoitettavissa useasta eri toimipisteestä.

Halusin toteutuksen olevan helposti toistettavissa jollekin toiselle asiakkaalle, tinkimättä minkään osapuolen omaisuudenhallinnasta, tietoturvasta tai ylläpidettävyydestä. Näistä syistä päädyin toteuttamaan moniasiakasympäristöön soveltuvaa palvelinalustaa, mistä voisin tarjota julkisia tai yksityisiä palvelinkokonaisuuksia. Tmi M Designille tämä tarkoittaa etäyhteyksillä toteutettua yksityistä verkkoa, jonne asennettaan virtuaalipalvelimelle www-pohjainen salasanojen hallintajärjestelmä.

Työssä käydään läpi tarvittavat komponentit ja periaatteet tällaisen yhteyden toteuttamiseksi, alkaen asiakkaan asiakasohjelmasta ja päättyen virtualisointialustaan palvelinlaitteiston päällä. Työn tavoitteena on toimittaa kokonaisuus, jotta asiakas voisi keskittyä omaan ydinosaamiseensa.

1.3 Osista kokonaisuuksiin

Työn keskiössä on kolme eri virtuaalikomponenttia: virtuaalinen erillisverkko (VPN, Virtual Private Network), virtuaalilähiverkko (VLAN, Virtual Local Area Network) ja palvelinvirtualisointi. Nämä kolme yhdistämällä on mahdollista tarjota usealle täysin eri maanosassa ja organisaatioissa oleville eri toimijoille omia yksityisiä palvelinratkaisuja yhdellä keskitetyllä palvelinlaitteistolla. Palvelinvirtualisoinnilla voidaan jakaa laitteiston resurssit eri virtuaalikoneille, joita käyttävät eri organisaatiot. Virtualisoitujen käyttöjärjestelmien suoritusympäristöt on eriytetty toisistaan joten niillä olevat tiedot eivät voi vuotaa ulos omasta järjestelmästä (kuvassa 1: VM-A). Palvelinlaitteisto on kytketty hallittavaan kytkimeen, joka mahdollistaa virtuaalilähiverkkojen käytön.



Kuva 1. Suunnitelma lopputuloksesta

Virtuaalilähiverkoilla saavutetaan verkkoliikenteen erottelu lähiverkkotasolla, jolloin eri organisaatioiden palvelimet voivat turvallisesti kommunikoida verkkoon huolehtimatta samalla laitteistolla ajettavista muista virtuaalipalvelimista (kuvassa 1: VLAN A). Jotta organisaatio voisi parhaalla mahdollisella tavalla hyödyntää näitä virtualisoituja palvelinresursseja, tarvitaan vielä siirtotie organisaation omasta lähiverkosta palvelinverkkoon. Tähän tarkoitukseen on virtuaalinen erillisverkko, jonka avulla voidaan reitittää kaksi lähiverkkoa julkisen Internetin yli.

Virtuaalinen erillisverkko luodaan palveluntarjoajan palomuurin ja organisaation palomuurin tai reitittimen välille (kuvassa 1: VPN A). Liikenne kulkee salattuna ja uudelleenpaketoituna julkisessa verkossa ja puretaan VPN-reitittimellä. Näin molempien lähiverkkojen resurssit ovat täysin käytettävissä. Ilman virtuaalista erillisverkkoa kummaltakin puolelta näkyisi vain reunalaitteen julkinen IP-osoite (Internet Protocol).

2 Virtuaalinen erillisverkko

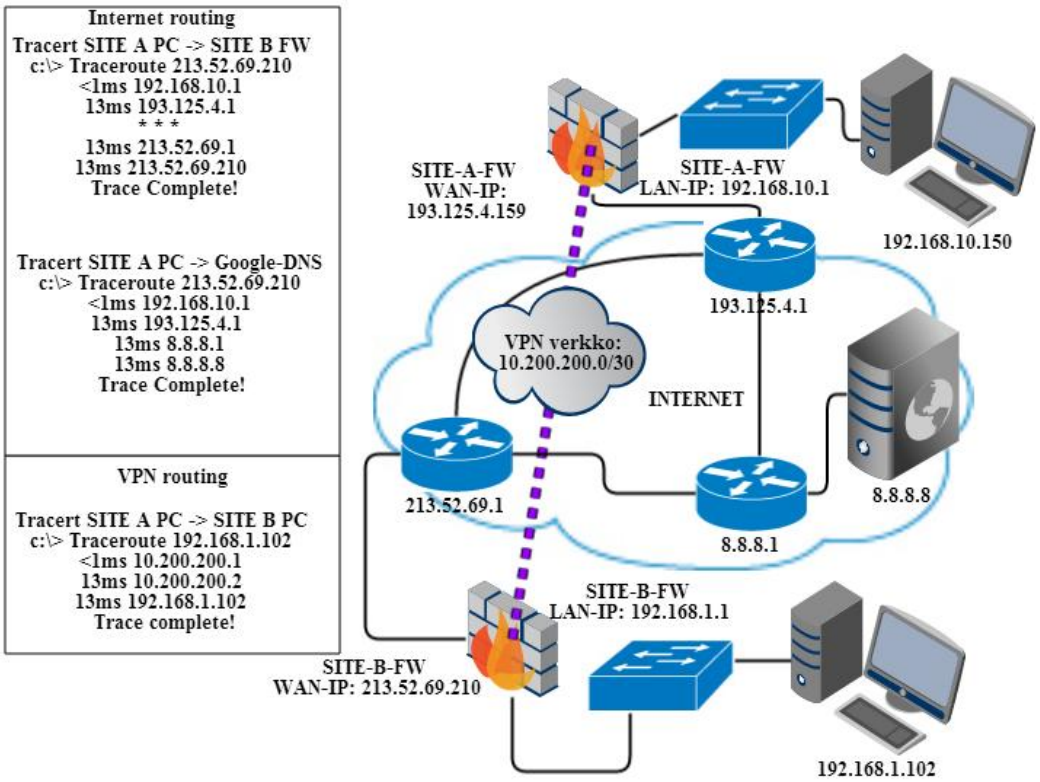
2.1 Virtuaalisen erillisverkon perusteet

Virtuaaliset erillisverkot tunnetaan paremmin nimellä VPN. Oli kyseessä sitten VPN-verkko tai VPN-yhteys, niin määritelmä on hyvin laajasti ja vapaamuotoisesti käytössä. Yksinkertaisesti selvennettynä virtuaalinen erillisverkko on yksityinen verkko, joka on rakennettu yhteisen verkkoinfrastruktuurin, kuten Internetin, päälle. Virtuaalista erillisverkkoa käytetään yhdistämään ja salaamaan kahden erillisen lähiverkon liikenne, kun sitä ei voida tehdä OSI-mallin (Open Systems Interconnection Reference Model) L2- tai L3-tasolla, eli verkon siirtokerroksella (L2) kytkemällä verkkoja yhteen kytkimen avulla tai verkkokerroksella (L3) eli reitittämällä verkkoja reitittimen avulla [1.]

IPsec (IP Security Architecture)-protokollaan perustuvat VPN-yhteydet ovat L3-tason yhteyksiä, jotka toteutetaan verkkokerroksella. IPsec on kombinaatio monesta RFC:stä (Request for Comments IETF-organisaation (Internet Engineering Task Force) julkaisemia Internetiä koskevia standardeja), ja se määrittelee kaksi pääasiallista protokollaa käytettäväksi [14]: AH (Authentication Header) ja ESP (Encapsulating Security Payload). ESP on suositeltu valinta, sillä se tarjoaa sekä todentamisen että yksityisyyden [2]. IPsec tarjoaa toiminnot, joilla voidaan tunnistaa yksittäiset IP-paketit ja varmistaa, että ne ovat muokkaamattomia, salata IP-paketin sisältämä data sekä kapseloida virtuaali-

sen erillisverkon kahden päätepisteen välinen salattu liikenne. IPsec tarjoaa ainoastaan vastapään osoitteen varmennuksen, minkä takia sitä käytetäänkin lähinnä verkkolaitteiden välillä kiinteiden tunnelien luomiseen [3.]

OpenVPN-protokollaan perustuvat VPN-yhteydet ovat L4-tason yhteyksiä, jotka käyttävät erityistä SSLv3 (Secure Sockets Layer)/TLSv1:een (Transport Layer Security) perustuvaa salausmenetelmää. Tiedonsiirron salaus tapahtuu siis OSI-mallin kuljetuskerroksessa (L4) TCP-(Transsmission Control Protocol) tai UDP (User Datagram Protocol) -protokollan päällä. OpenVPN käyttää tiedonsalaukseen OpenSSL-kirjastoa sekä tiedonsiirron että hallintakanavan liikenteen salaamiseen. Käyttäjän tunnistukseen OpenVPN tarjoaa mahdollisuudeksi esijaettua avainta, sertifikaattia tai käyttäjätunnus-salasanaparia. Tämä tekee OpenVPN:n protokollasta erityisen joustavan ratkaisun, sillä se soveltuu helposti käytettäväksi kiinteissä tunneleissä sekä myös mobiiliyhteyksissä (remote access). Mobiiliyhteydet luodaan suoraan käyttäjän koneelta käyttäen erillistä yhteysohjelmaa, jolloin joissakin tapauksissa niihin viitataan L4/L7-yhteyksinä [4;5.]



Kuva 2. Havainnekuva erillisverkosta.

Kuvasta 2 voi nähdä yleisellä tasolla, kuinka VPN-yhteydellä liikenne kulkee salattuna kahden VPN-yhteyspisteen välillä, eikä julkisen verkon reitityspisteitä VPN-käyttäjän näkökulmasta oteta huomioon. Näin voidaan turvallisesti reitittää kaksi lähiverkkoa julkisen Internetin kautta.

2.2 Sertifikaatit ja jaetut avaimet

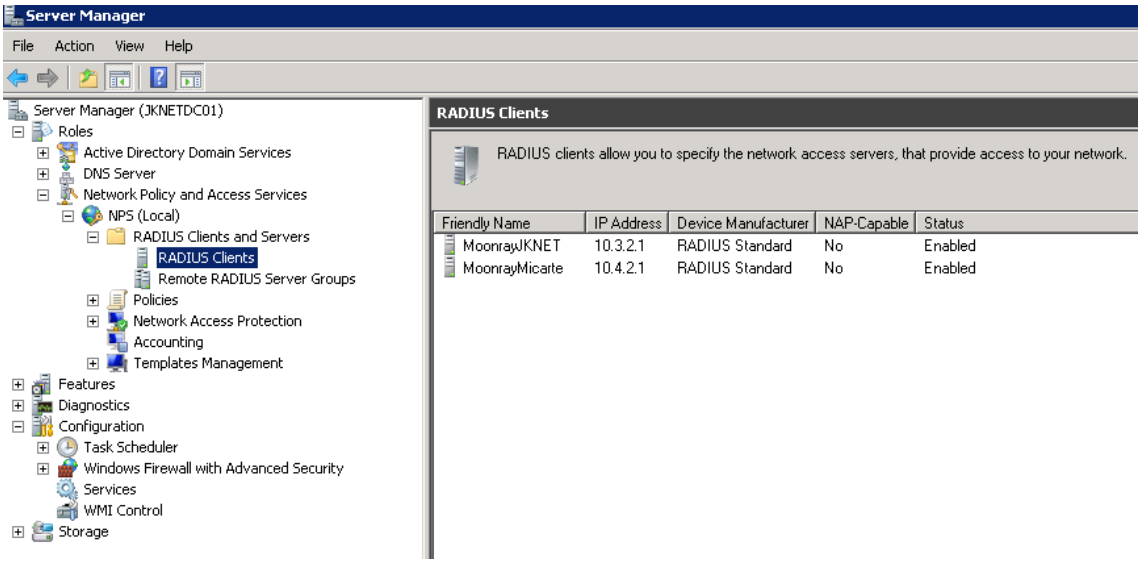
Sertifikaatti on sähköinen dokumentti, joka käyttää digitaalista allekirjoitusta yhdistämään julkinen avain johonkin tahoon, kuten Internet-sivustoon, sähköpostin lähettäjään tai VPN:n käyttäjään. Tällaisia julkisia avaimia allekirjoittaa sertifikaatin myöntäjä. Suuremmissa yrityksissä sisäiset palvelut varmennetaan sertifikaateilla, jotka allekirjoitetaan oman infrastruktuurin sertifikaatin myöntäjällä. Sertifikaatin myöntäjän oma varmenne asennetaan jokaiselle koneelle luotettujen myöntäjien listaan niin sanotuksi juurivarmenteeksi. Tällaisia juurivarmenteita on muitakin, ja niitä tarvitaan erityisesti Internet-sivuilla, missä ei voi olla vain yhtä toimijaa, johon kaikki luottaisivat. Suuremmat yritykset ovat voineet hakea sertifikaatin myöntäjän roolia, jolloin niiden julkinen avaimensa eli juurivarmenteensa laitetaan valmiiksi useisiin käyttöjärjestelmiin, sekä selaimiin. Näiltä sertifikaatin myöntäjiltä haettuihin julkisiin avaimiin voi siis useampi käyttäjä luottaa ilman riippuvuuksia jonkun organisaation asennuskäytäntöihin. Sertifikaatin myöntäjät ylläpitävät myös sertifikaatin peruutuslistaa, josta voidaan tarkistaa, onko kyseinen sertifikaatti mahdollisesti hylätty jo sen varsinaisen voimassaoloajan aikana [20.]

Jaettu avain on tarkoitukseltaa hieman samantyyppinen, mutta sitä ei ole erikseen varmennettu miltään taholta. Se on kahden eri toimijan yhdessä sopima salainen merkkijono, jota käytetään yhteyden muodostamisvaiheessa. Esimerkiksi IPsecin tilanteessa toinen päätepiste lähettää salatun viestin, joka sisältää jaetun avaimen, ja jos vastapuoli pystyy itsenäisesti luomaan samanlaisen salatun viestin käyttäen itselleen määriteltyä jaettua avainta, niin se tietää, että molemmilla laitteilla täytyy olla sama jaettu avain. Näin muodostuu salattu yhteys kahden päätepisteen välille [21.]

2.3 Käyttäjän todentaminen

Käyttäjien todentamiseen voidaan käyttää edellä mainittujen tapojen lisäksi käyttäjätunnusta ja salasanaa. Tätä varten tarvitaan käyttäjätunnus- ja salasanatietokanta. Monissa palomuurijakeluversioissa tämä on mahdollista toteuttaa paikallisesti. Jos näitä paikallisia tietokantoja ei voi luoda useita tai jakaa käyttäjiä ryhmiin, niin kaikki tietokantaan määritellyt käyttäjätunnus-salasanaparit pääsevät kirjautumaan kaikkiin laitteeseen määriteltyihin VPN-instansseihin.

Toinen vaihtoehto on hyödyntää olemassa olevaa Windows-toimialueen aktiivihakemistoa käyttäjien todennukseen. Tämä onnistuu asentamalla Windows-palvelimelle *Network Policy and Access Services* -rooli ja määrittelemällä siihen RADIUS (Remote Authentication Dial In User Service) -palvelu. RADIUS-palveluun määritellään tarvittavat vaatimukset, joiden perusteella voidaan sallia kirjautuminen palvelun kautta. Näihin vaatimuksiin voisi kuulua esimerkiksi jäsenyys johonkin tiettyyn ryhmään. RADIUS-asiakkaan, joka tässä tapauksessa on VPN-palomuuri, osoite täytyy määritellä, jotta RADIUS-palvelu tietää pyynnön tulevan luotetulta taholta. Lisäksi molempiin pitää määritellä jaettu avain salasanaksi. Kuvassa 3 on esillä RADIUS-asiakkaat, jotka ovat siis yhdyspisteitä, joiden kautta päätelaitteet tunnistautuvat verkkoon. Kyseessä voi siis olla esimerkiksi langattoman verkon tukiasema tai VPN-yhteyspiste. Kuva 3 esittää RADIUS-palvelun asiakasnäkymää, johon on määritelty kahdesta eri IP-osoitteesta tulevat pyynnöt eri RADIUS-asiakkaiksi [16.]



Kuva 3. Windows palvelimen RADIUS palvelun asiakasnäkymä.

2.4 Asiakasyhteyksien toteutus

Työn toteutukseen olen valinnut VPN-reitittimeksi ja palomuuriksi avoimeen lähdekoodiin perustuvan pfSense-järjestelmän.

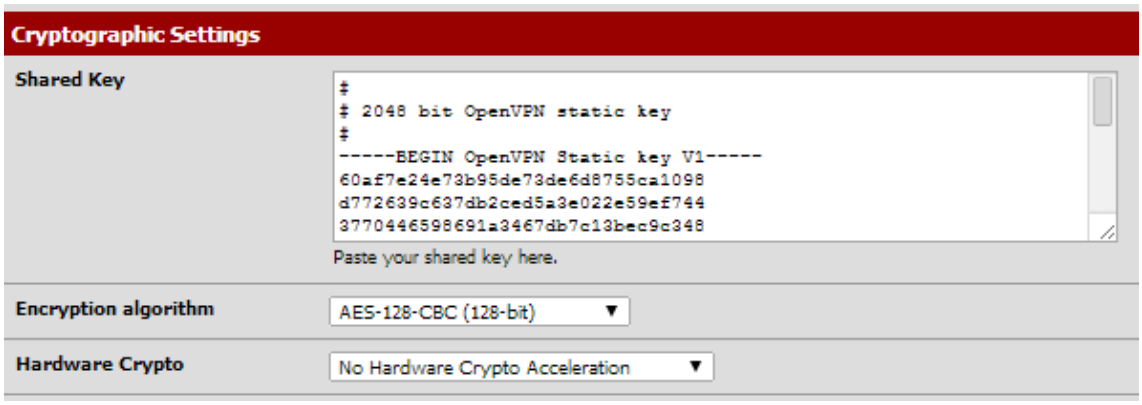
pfSense-projekti on BSD (Berkeley Software Distribution)-käyttöjärjestelmään pohjautuva palomuurijakeluversio omalla muokatulla kernelillä eli käyttöjärjestelmän ytimellä. Mukana tulee myös kolmannen osapuolen sovelluksia, joilla järjestelmän ominaisuuksia voidaan laajentaa. pfSense on vapaasti ladattavissa ja asennettavissa monen tyyppisille alustoille. Sitä voi testata Live CD:ltä (Compact Disc), asentaa palvelinlaitteistolle, Flash-kortille johonkin sulautetun järjestelmän laitteiseen tai mille tahansa tältä väliltä. Hallinta on mahdollista kaikkien komponenttien osalta www-hallintaliittymän kautta, eikä aikaisempaa tuntemusta BSD käyttöjärjestelmistä tarvita [2.]

Valitsin pfSensen tähän työhön sen monipuolisten VPN-toimintojen perusteella, ja koska minulla oli siitä aikaisempaa kokemusta. PfSensen VPN-ominaisuuksiin kuuluvat IPsec, OpenVPN, PPTP (Point-to-Point Tunneling Protocol) ja L2TP (Layer 2 Tunneling Protocol). Näistä hyödyllisimmät toteutukseen ovat IPsec ja OpenVPN, koska niitä olen nähnyt eniten käytettävän yrityksien reunalaitteilla ja ne ovat ainoat yhteysmuodot, joista voidaan luoda useita instansseja yhdelle laitteistolle. PPTP on jo poistumassa oleva yhteystapa, sillä sitä on alettu pitämään turvattomana [15]. L2TP voi osoittautua tarpeelliseksi joissakin tapauksissa, jos esimerkiksi mobiililaitteisiin ei voida asentaa OpenVPN-asiakasohjelmaa, sillä suurimmissa mobiilialustoissa on natiivi L2TP VPN-yhteyksien tuki. IPsec tarjoaa laajan tuen muiden valmistajien tuotteiden kanssa muodostettaviin VPN-tunneleihin (mm. Cisco, Juniper). OpenVPN tarjoaa hyvän tuen moniin muihin palomuurijakeluversioihin muodostettaviin VPN-tunneleihin, sekä erinomaisen mobiilikäyttäjien tuen. Kolmannen osapuolen sovelluksella OpenVPN-palvelimien asiakasohjelmat saa tallennettua suoraan joko asennettavana pakettina, pelkkinä asiakasohjelman asetustiedostoina tai sulautettuna tiedostona, jossa on asetukset ja sertifikaatti älypuhelimille tai tableteille.

Tällä hetkellä palomuurissani on käytössä vain OpenVPN. Siinä on kaksi kiinteää tunnelia ja kolme mobiilikäyttäjiä varten määriteltyä OpenVPN-palvelininstanssia. Jokaiselle asiakkaalle tulee oma OpenVPN-palvelininstanssi, jonne määritellään kyseisen verkon IP:t, salausmäärittelyt, käyttäjäntunnistustapa (paikallinen tai RADIUS), mistä portista palvelu kuuntelee saapuvia yhteyksiä ja mitä verkkoja tunneliin reititetään [4.]

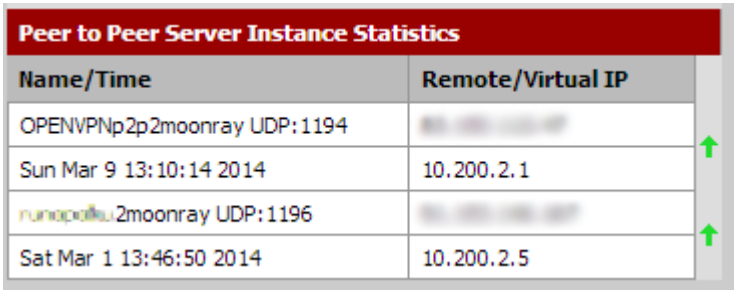
Kiinteät yhteydet

Työn aikana palvelinsaliin on toteutettu kaksi kiinteää VPN-tunnelia, käyttäen OpenVPN-protokollaa. Kuvassa 4 on esitettynä osa asetussivusta. Kuvassa on määriteltynä automaattisesti luotu jaettu avain.



Kuva 4. Kiinteän tunnelin salausasetukset.

Käytössä on yhdyspisteestä yhdyspisteeseen yhteys 2048-bittisellä jaetun avaimen todentamisella. Liikenne salataan AES-128-CBC-algoritmilla. OpenVPN-tunneleiden etuna on myös helpompi reititys tunneleiden takana oleville verkoille. verrattuna esimerkiksi IPsec tunneleihin. OpenVPN-tunnelin palvelinpään asetuksiin määritellään palvelimen takana sijaitsevat verkot sekä asiakaspään takana olevat verkot. Näin OpenVPN osaa automaattisesti lisätä reitit näihin verkkoihin palomuurin reititystauluun, sekä palvelimen että asiakkaan päässä.



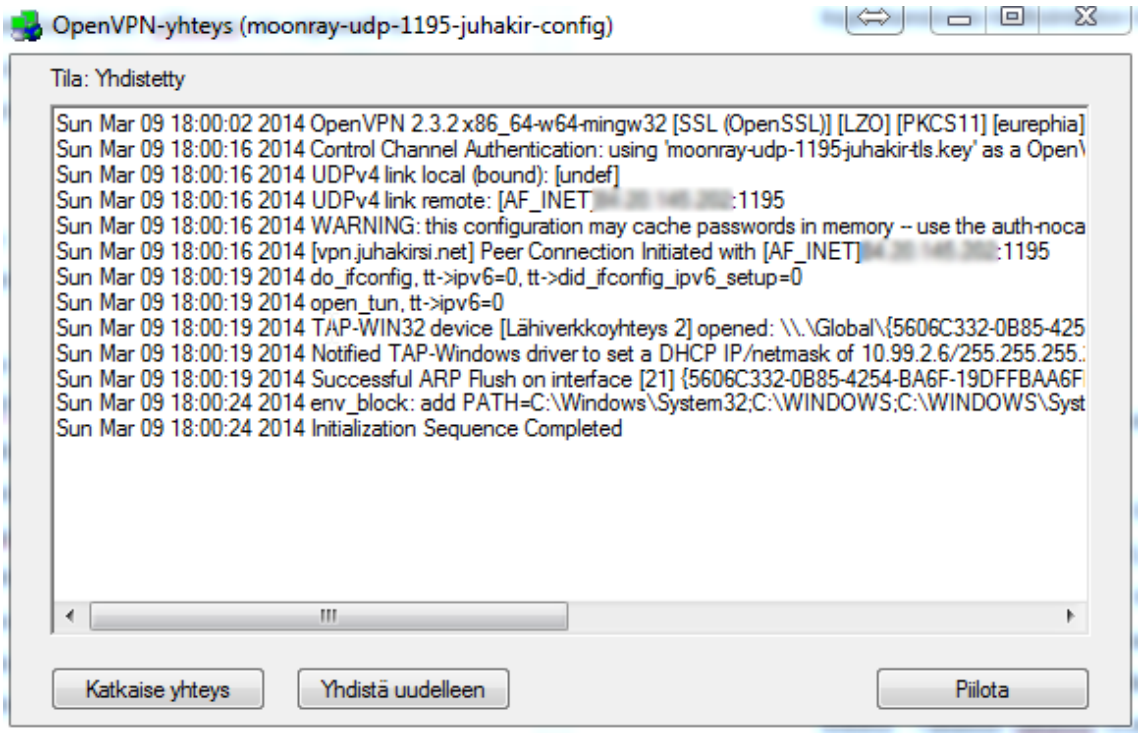
Kuva 5. Kiinteät OpenVPN-tunnelit.

Kuvassa 5 näkyy palvelinsalin palomuuriin muodostetut kiinteät VPN-yhteydet. Ensimmäinen tunneli on tehty vasten omaa palomuuriani kotitoimistolla. Sieltä käsin tapahtuu päivittäinen ylläpito- ja asennustyöt virtuaalijärjestelmään. Tunnelin kautta ajetaan myös jokaöiset varmuuskopiot palvelinsalin levyjärjestelmän varmuuskopiokansiosta kotitoimiston levyjärjestelmään.

Mobiilit yhteydet

Mobiilit yhteydet palvelimeen on tuotettu käyttäen OpenVPN-palvelininstansseja. Yksi palvelininstanssi vastaa yhtä kuuntelevaa porttia palvelimella. Jokaiselle asiakasorganisaatiolle luodaan oma palvelininstanssi, johon määritellään käyttäjäntodennustapa. Sopivin tapa on käyttää asiakkaan omaa Windows aktiivihakemistopalvelinta (AD, Active Directory) RADIUS-palvelimena, jolloin käyttäjät voivat käyttää oman organisaationsa käyttäjätunnusta ja salasanaa. Palomuuriin on myös mahdollista luoda paikalliset tunnukset käyttäjien todentamista varten.

Tämän lisäksi luodaan TLS-varmistusta varten 2048-bittinen staattinen avain, valitaan juurivarmenteen myöntäjä, joka monessa tapauksessa on palomuurin oma juurivarmenne. Palvelimen varmenteenmyöntäjällä tehty sertifikaatti, joka on luotu organisaatiota varten, valitaan palvelinsertifikaatiksi. Diffie Hellman avaimenvaihtoparametrien valinta ja salausalgoritmin valinnat voi jättää oletusasetuksille käyttöjärjestelmän toimittajan suosituksen muokaisesti. Seuraavaksi määritellään IP-verkko tunnelia varten. Pienen yrityksen verkoksi riittää 28-bittinen verkko, jolloin siinä on myös laajennusvaraa, jos käyttäjämäärä äkillisesti kasvaisi. Tällaisessa verkossa on käytettävissä 14 osoitetta, joista käyttäjät saavat virtuaalisen IP:n koneellensa tunneliverkkosovittimeen. Liikenne tunneliverkkoon ja palomuurin takana oleviin verkkoihin näkyy tällä IP:llä palomuurissa, joten sen perusteella tehdään palomuurin säännöt. Palomuurisääntöjen lisäksi pääsyä kannattaa rajoittaa mainostamalla tunneliin ainoastaan ne verkot, jotka kyseisen verkon kautta halutaan olevan tavoitettavissa.



Kuva 6. OpenVPN-GUI asiakasohjelman tilaikkuna.

Kun palvelininstanssin asetukset on määritelty, voi asiakaspaketin ladata kolmannen osapuolen paketilla ”*Client Export Utility”.* Tarjolla on latauslinkki jokaiselle palvelininstanssille ja niiden käyttäjille. Jokaiselle ympäristölle on oma asennuspaketti tai asetustiedostopaketti. Kuvassa 6 näkyy tällaisen asiakasohjelman tilanneikkuna yhteyden muodostuksen aikana.

Tmi M Designilla on OS X:n käyttäjiä, joten heille on toimitettu Viscosity-ohjelmaan räätälöidyt asetustiedostot. Viscosity on Apple OS X:n käyttäjille suunnattu OpenVPN-asiakasohjelma, jolla luodaan mobiili VPN-yhteys. Tunnistautuminen tapahtuu heidän toteutuksessaan omalta Windows-palvelimelta, jonne on määritelty ryhmät ja käyttäjät aktiivihakemistoon. RADIUS-palveluun on luotu tarvittavat säännöt käyttäjäntodentamispyyntöjen hyväksyntää varten.

3 Virtuaalilähiverkko

3.1 Virtuaaliähiverkon perusteet

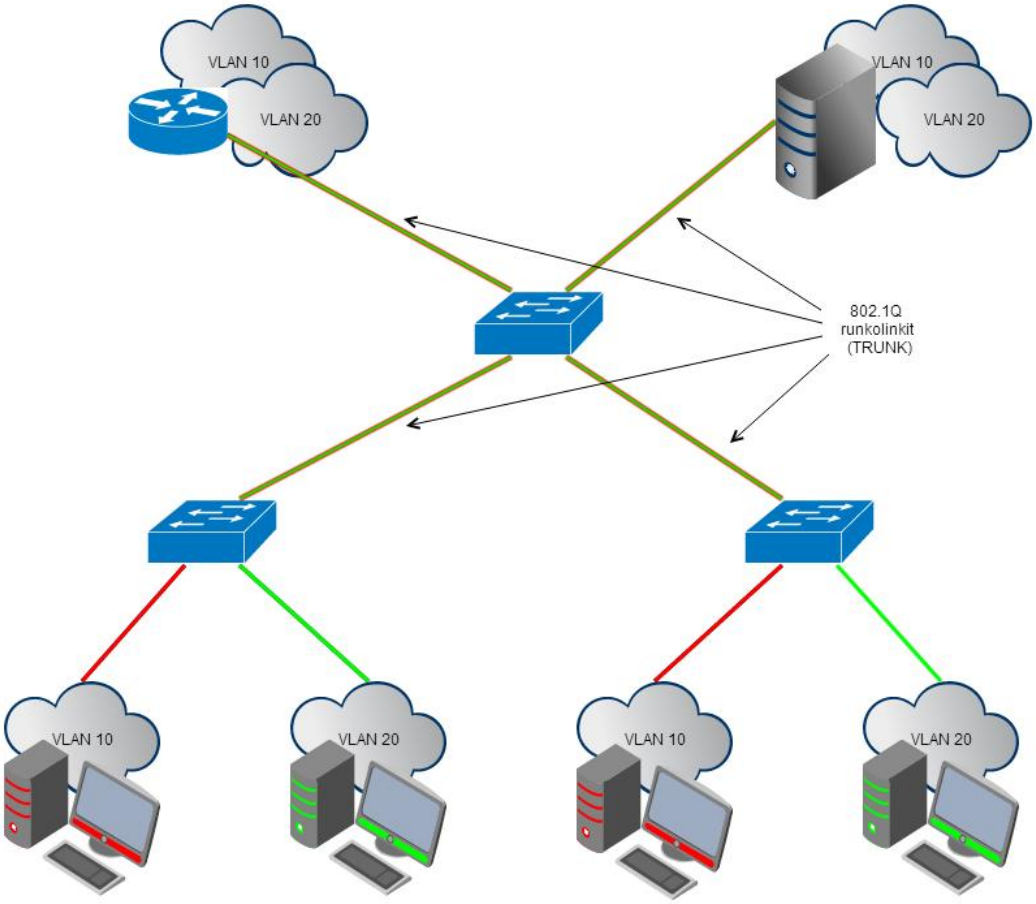
Virtuaalilähiverkko, lyhyesti VLAN, on fyysisen verkon loogisella jakamisella saavutettua verkon laajentamista. VLAN-tekniikalla voidaan hyödyntää yhtä fyysistä mediaa, kuten ethernet-parikaapelia, tehokkaammin yhdistämällä useita erillisiä verkkoja. VLAN-tekniikka ei kasvata kuitenkaan kaistanleveyttä, joten jos liikennemäärät ovat suuria, tarvitaan muita verkkotekniikoita fyysisten linkkien yhdistämiseksi yhdeksi loogiseksi linkiksi. Tällaisia ovat mm. LACP (Link Aggregation Control Protocol) tai EtherChannel, jotka kokoavat kytkimen porttiryhmiä yhdeksi loogiseksi portiksi. Käytännössä siis esimerkiksi henkilöstöhallinto, taloushallinto ja myynti voidaan erotella omiin loogisiin osiinsa verkossa riippumatta osastojen fyysisestä sijainnista.

VLAN-tekniikka vaatii tuen kytkimiltä ja reitittimiltä. Virtuaalilähiverkkoja tukevat laitteet lisäävät verkkoliikenteen paketteihin VLAN-otsikon, joka on 32-bittinen kenttä, jonka sisälle on määritelty VLAN-tunniste. Sen avulla vastaanottava laite tunnistaa liikenteen kuuluvan johonkin tiettyyn virtuaalilähiverkkoon. Tällainen liikenne on pääsääntöisesti verkon aktiivilaitteiden, kuten kytkimien tai reitittimien välistä liikennettä.

Kun vastaanottavassa päässä, ei ole laitetta, joka tukisi VLAN-otsikolla varustettuja paketteja, kuten työryhmäkytkimeen kytkeytyvä kannettava, poistetaan paketeista ulosmenevässä portissa VLAN-otsikko. Samoin kyseisestä portista sisään tulevat paketit, joissa ei ole VLAN-otsikkoa, voidaan portilla merkitä asianmukaisella otsikolla. Näistä porteista käytetään usein nimityksiä *tagged* ja *untagged*. Tagged tarkoittaa porttia, josta ulos lähtevä liikenne merkitään otsikolla ja untagged tarkoittaa porttia, josta otsikot poistetaan. Yhteen porttiin voidaan määritellä vain yksi VLAN untagged-tilaan, mutta useita VLANeja tagged-tilassa. Porttia, joka kuljettaa eteenpäin tagged tilassa kaikkia kytkimen tuntemia VLANeja, kutsutaan *runko*portiksi (TRUNK-port). VLAN-tekniikan standardit on määritelty IEEE 802.1Q-standardilla, jolla varmistetaan eri laitevalmistajien välinen yhteensopivuus [5.]

VLAN-verkon sisällä on yksi IP-aliverkko, jonka sisällä eri käyttäjät voivat kommunikoida vapaasti, mutta eri VLANien välillä liikenne ei ole mahdollista ilman reititystä [3.]

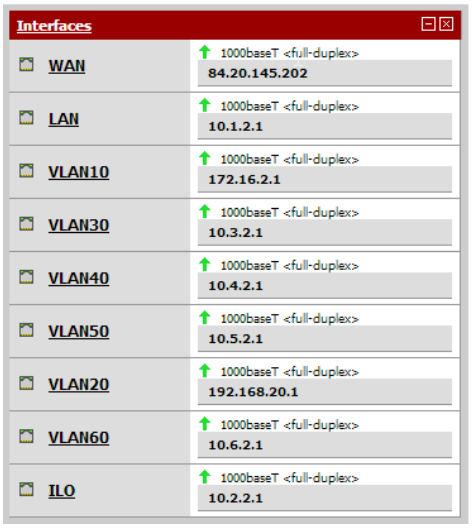
Kuvassa 7 on esitettynä lähiverkko, joka on jaettu kahteen eri VLANiin. Palvelin on liitettynä molempiin VLAN-verkkoihin, jotta molempien verkkojen työasemat pääsevät sen resursseihin kiinni. Reititin mahdollistaa eri VLAN-verkoissa olevien työasemien keskinäisen kommunikoinnin.



Kuva 7. VLAN-havainnekuva.

3.2 Virtuaalilähiverkon toteutus

Toteutuksessa VLAN-tekniikka on avaintekijä, jotta yhdestä järjestelmäkokonaisuudesta voidaan tarjota palveluja useammalle eri taholle. VLANit määritellään pfSense-palomuurissa ja niille määritellään virtuaalinen liitäntäpiste (Kuva 8) (*VLAN interface*), jonka perusteella voidaan palomuuriin määritellä palomuurisääntöjä liikenteen rajoittamiseksi (Kuva 9). Omassa toteutuksessani ovat VLANit 10, 20, 30, 40, 50, 60 sekä 911.



Kuva 8. VLAN-liitännät.

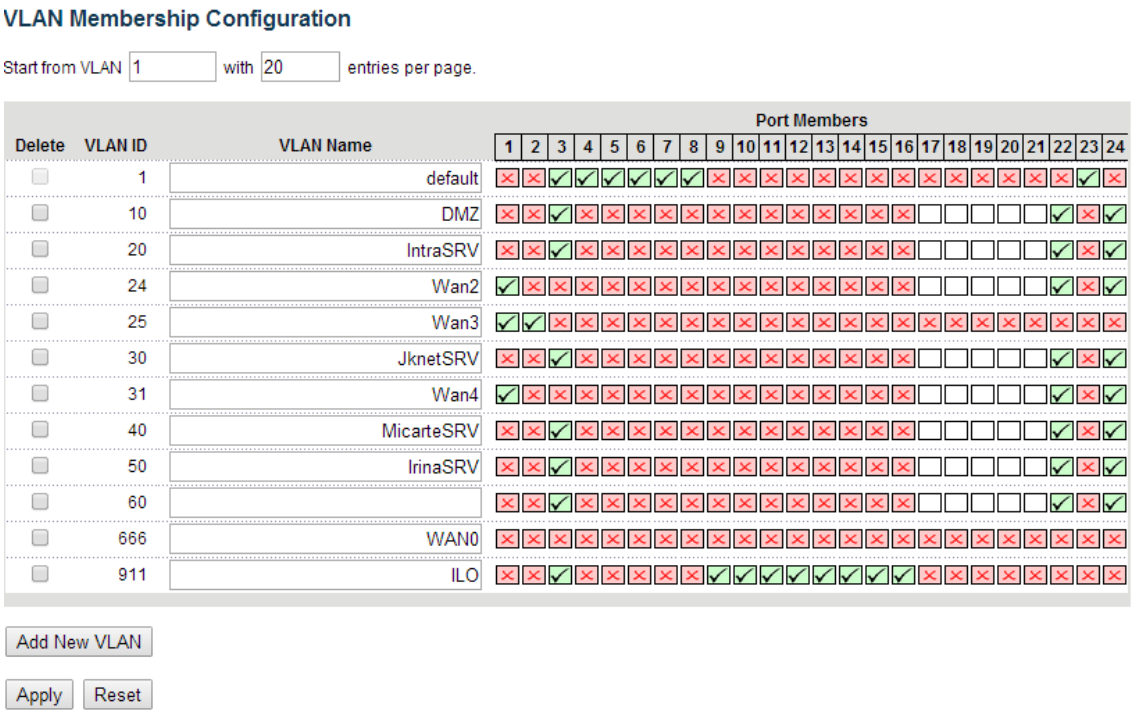
Näiden käyttötarkoitus on seuraavanlainen. VLAN 10 on DMZ (Demilitarized Zone)-verkko, eli verkko, jonne sijoitetaan palvelut, joihin tarjotaan pääsy palomuurin ulkopuolelta. VLAN 20 on sisäinen jaettu intrapalvelinverkko itselle ja kumppaneille. VLAN 30 on omien palveluiden käytössä ja loput ovat eri asiakkaiden omia verkkoja.

Käytännössä yhdellä VLANilla on oma IP-aliverkko. Tällä hetkellä näihin on allokoitu kokonaiset 24-bittiset verkot, jotka tullaan pilkkomaan huomattavasti pienemmiksi verkoiksi tarpeen mukaan. Yhdelle asiakkaalle ei ole järkevää allokoida 254:ää IP-osoitetta yhtä palvelinta varten. Esimerkiksi pienyrityksen tarpeisiin voisi riittää jopa /29-verkko, jossa olisi tilaa 5:lle palvelimelle. Näiden hallintaan tarvitaan toki jo jonkinlainen IP-osoitteiden hallintapalvelu (IPAM, IP Address Management).

Kuva 9. Palomuurisäännöt VLAN 10:lle.

Palomuurilta nämä VLANit liikennöivät sisäverkoon LAN-portista ethernet-kaapelia pitkin kytkimelle, joka tässä tapauksessa on 24-porttinen Zyxelin hallittava gigabittinen

kytkin. Kyseistä kytkintä hallitaan Internet-selaimella SSL-suojatulta sivulta. Jokaiselle portille määritellään, minkä VLANien liikennöintiin portti osallistuu. Koska tämä on tagged-VLAN-valinta, voidaan yhdelle portille määritellä useita VLANeja. Sen lisäksi on Port VLAN, joka on siis untagged VLAN-valinta, ja se voi olla vain yksi tietty VLAN-numero.



Kuva 10. Porttien tagged-VLAN-määritykset.

Kuva 10 näyttää, miten hallintaliittymän kautta on merkitty vihreällä sallitut VLAN-numerot ja punaisella estetyt VLAN-numerot. Estetyillä VLAN-numeroilla on Zyxelin tapauksessa merkitystä lähinnä, jos portti määritellään runko-portiksi kahden kytkimen välille. Näin voidaan rajata joku tietty verkko pois toiselta kytkimeltä.

Samat määritykset voidaan toteuttaa myös komentorivipohjaisilla kytkimillä, kuten Ciscon tai HP:n kytkimillä. Vastaavat määritykset Ciscolla tehtäisiin seuraavilla komennoilla, esimerkiksi porttiin GigabitEthernet 0/1

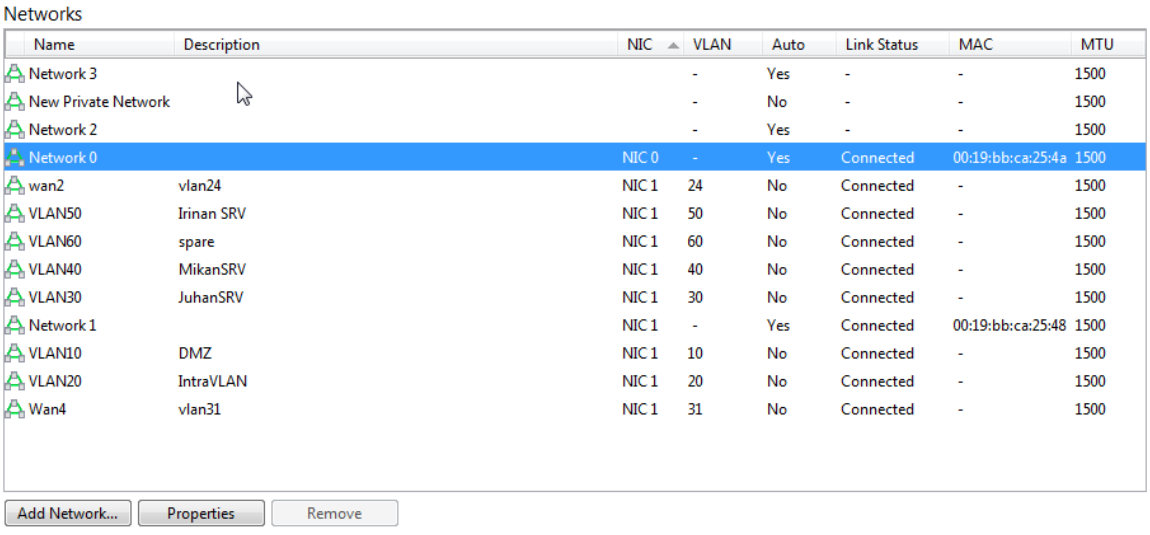
```
>enable
#configure terminal
(config)#interface GigabitEthernet0/1
(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport trunk allowed vlan 24-25, 31
(config-if)#switchport mode trunk
```

Tarvittaessa, jos halutaan porttiin vielä jokin untagged VLAN (esimerkissä vlan10), voidaan antaa seuraava komento:

```
(config-if)#switchport trunk native vlan 10
(config-if)#end
#wr
```

Lopuksi poistutaan asetusmäärittelytilasta ja kopioidaan asetukset NVRAM (Non-Volatile Random Access Memory)-muistiin, jotteivät asetukset häviä kytkimen uudelleenkäynnistyksessä.

Kytkimeltä VLANit kuljetetaan itse palvelimelle, jonka käyttöjärjestelmänä toimiva virtualisointialusta on VLAN-kykyinen. Virtualisointialustalla on oma virtuaalinen kytkin, josta virtuaalikoneet kytketään haluttuun VLANiin. Koska kyseessä olevalla palvelinlaitteella ajetaan useita virtualipalvelimia eri VLANeissa, pitää portti määritellä Ciscossa runkoportiksi tai Zyxelillä määritellä tarvittavat VLANit kyseiseen porttiin kuuluviksi *tagged*-VLAN-porteiksi. Jos olisi kyseessä perinteinen palvelin, riittäisi Zyxelin port-VLAN-määritys tai Ciscossa *#switchport mode access* ja *#switchport access vlan [numero].* Näin portista tapahtuva liikennöinti olisi *untagged*-tyyppistä, eikä palvelimeen tarvitse erikseen määritellä VLAN-ominaisuuksia. Kuvassa 11 on esitettynä XenCenter-hallintaohjelman näkymä virtuaalialustalle määriteltyihin VLAN-verkkoihin.



Kuva 11. XenCenterin verkonhallinta.

4 Palvelinvirtualisointi

4.1 Palvelinvirtualisoinnista

Palvelinvirtualisoinnilla tarkoitetaan fyysisen palvelinlaitteiston piilottamista virtualisointikerroksen alle. Virtualisointikerroksen päällä voidaan ajaa useita käyttöjärjestelmiä yhtä aikaa yhdellä laitteistolla niiden häiritsemättä toisiaan. Tämä on toteutettu käyttämällä prosessorille eri suojaustasoja ja jakamalla virtuaalikoneille dynaamisesti omat muistialueet. Näin virtuaalikoneen antaessa esimerkiksi uudelleenkäynnistyskomennon se toteutetaan vain kyseiselle virtuaalikoneelle, eikä varsinaiselle isäntälaitteelle.

Perinteisten palvelimien, joita on asennettu erikseen jokaista sovellusta varten, tehojen kuormitus on yleensä ollut 10–15 %:n luokkaa. Ne ovat vieneet paljon tilaa palvelinkeskuksissa, kuluttaneet paljon sähköä ja tuottaneet paljon lämpöä, jonka poistamiseen tai viilentämiseen on jouduttu käyttämään paljon energiaa. Laitteiston jäähdyttämiseen ja toiminnan pyörittämiseen kuluu merkittävä osa yrityksen energiankäytöstä. Virtualisointia voidaan pitää ekotekona; fyysisen laitteiston määrän ja näin ollen tarvittavan energian määrän pienentyessä myös yrityksen hiilijalanjälki pienenee.

Laitteiston huoltotoimenpiteet ovat myös helpompia, koska virtualisoidut palvelimet voidaan siirtää toiselle laitteistolle huoltotoimenpiteiden ajaksi. Palvelimien palvelutaso on siis kasvanut merkittävästi, kun niitä ei tarvitse sammuttaa suunniteltujen laitteistohuoltojen takia. Resurssien lisääminen on virtualisoinnin ansiosta mahdollista asetuksia muuttamalla, ja se vaatii korkeintaan virtuaalikoneen uudelleenkäynnistämisen.

Virtualisointia on kolmea eri tyyppiä: käyttöjärjestelmätason virtualisointia, laitteistotason virtualisointia ja paravirtualisointia. Näistä palvelinvirtualisointiin käytetään lähinnä kahta viimeistä. Käyttöjärjestelmätason virtualisointituotteet, kuten VMware Player ja Workstation tai Oracle VM VirtualBox, ovat ohjelmistoja, jotka toimivat olemassa olevan käyttöjärjestelmän päällä virtualisointialustana. Virtualisoidut koneet ovat eriytettyjä isäntäkoneen käyttöjärjestelmästä. Tämän tyyppinen virtualisointi tukee kaikkia käyttöjärjestelmiä ja nopeus on hyvin lähellä isäntäkoneen nopeutta.

Laitteistotason virtualisoinnissa virtuaalikone näkee virtuaalisen laitteiston täysin samanlaisena kuin se on isäntälaitteessa eikä virtuaalikäyttöjärjestelmään tarvita erillisiä lisäohjelmia. Tästä johtuen tekniikalla on erittäin hyvä käyttöjärjestelmien tuki sekä te-

hokas prosessorin ja muistin hyödyntäminen. Laitteistotason virtualisoinnissa tarvitaan jokaiselle laitteelle oma ajuri ja siitä syystä virtualisointiohjelmistojen valmistajat usein listaavat yhteensopivat laitteet, joille asentamista tuetaan. Ilman tukea olevia laitteita ei välttämättä voida hyödyntää virtualisoinnissa.

Paravirtualisoinnissa isäntälaite ei emuloi suoraan palvelinlaitteiston komponentteja, vaan virtualisointialusta koordinoi pääsyä alla oleviin komponentteihin. Paravirtualisoinnissa virtuaalikoneiden vierellä ajetaan korotetuin oikeuksien hallintajärjestelmää, jolla on suora pääsy laitteistoon. Tässä sijaitsevat laiteajurit ja verkolaitteiden ohjaus sekä hallintarajapinta virtuaalikoneille. Paravirtualisointi vaatii vieraskäyttöjärjestelmään muokatun kernelin tai paravirtualisointia tukevat ajurit. [12, s. 67;11, s. 15-16]

4.2 Palvelinvirtualisoinnin toteutus

Vaihtoehdot

Projektin alkumetreillä lähdin suunnittelemaan ja testaamaan ideaa kahdella käytetyllä työasemalla. Ensivaiheessa virtualisointialustaksi valikoitui ProxmoxVE, joka on Debian-pohjainen avoimen lähdekoodin jakeluversio. ProxmoxVE yhdistää kaksi virtualisointitekniikkaa, joista OpenVZ hyödyntää käyttöjärjestelmävirtualisointia Linux-käyttöjärjestelmille. OpenVZ käyttää jaettuja resursseja ja mahdollistaa hyvin pienen muistinkäytön virtuaalikonetta kohden. Tämä on mahdollista siksi, että OpenVZ-järjestelmässä virtuaalikonetta ajetaan rinnakkain virtuaalialustan ytimen kanssa. Virtuaalikoneen täytyykin käyttää samaa versiota Linux-ytimestä, kuin mikä alustalla on käytössä. Järjestelmää käyttäen on siis mahdollista hyödyntää tehokkaasti hyvin pienilläkin resursseilla varustettuja koneita [17.]

Toinen tekniikka on KVM-virtualiasointi (Kernel Virtual Machine), joka on laitteistotason täysi virtualisointitekniikka. Se mahdollistaa muokkaamattomien Windows- ja Linux-käyttöjärjestelmien ajamisen [18.]

ProxmoxVE vaikutti hyvältä erityisesti kevyiden virtuaalisten Linux-säiliöiden takia, hyvin toimivien automaattisten varmuuskopioiden sekä hyvin toimivan käynnissä olevan virtuaalikoneen siirto-ominaisuuden vuoksi. Siinä oli kuitenkin suunniteltuun toteutukseen tarvittavassa ominaisuudessa merkittävä puute. Tuki virtuaalilähiverkoille oli puutteellinen hallintaliittymän puolella. Uusien virtuaalilähiverkkojen luominen vaati käyttä-

järjestelmän verkkokonfiguraatioihin muutoksia tiedostotasolla, eikä siihen löytynyt kattavaa dokumentaatiota. Ja koska virtualisointialusta ei vaikuttanut olevan erityisen tunnettu, ei myöskään yhteisön tarjoamasta tuesta löytynyt kaipaamaani laajaa kokemuspohjaa.

Tutkiessani muita avoimen lähdekoodin vaihtoehtoja, kävi selväksi että Xen-alustalla oli huomattavasti kehittyneimmät ominaisuudet. Vakuuttava VLAN-tekniikan ja verkonhallinnan mahdollistava käyttöliittymä oli yksi merkittävimmistä syistä valintaan. Lisäksi laaja käyttäjäkunta takaa, että ympäristöstä riittää kokemuksia ja tietoa ongelmien ratkaisuun.

Näistä syistä valitsin tähän toteutukseen Xen Projektin XCP v.1.6 (Xen Cloud Platform) -alustan, joka on viimeisimmän Citrix XenServer 6.2:n avoimen lähdekoodin vastine. Citrix XenServer 6.2 on mahdollista hankkia myös ilmaiseksi käyttöön, mutta siitä on rajattu käytöstä monia ominaisuuksia. Tällaisia ominaisuuksia ovat muun muassa automaattinen virtuaalikoneen varmennus ja palautus, käyttöasteen raportointi ja hälytys sekä käynnissä olevan virtuaalikoneen muistin tilannekuva ja palautus.

Oma toteutukseni

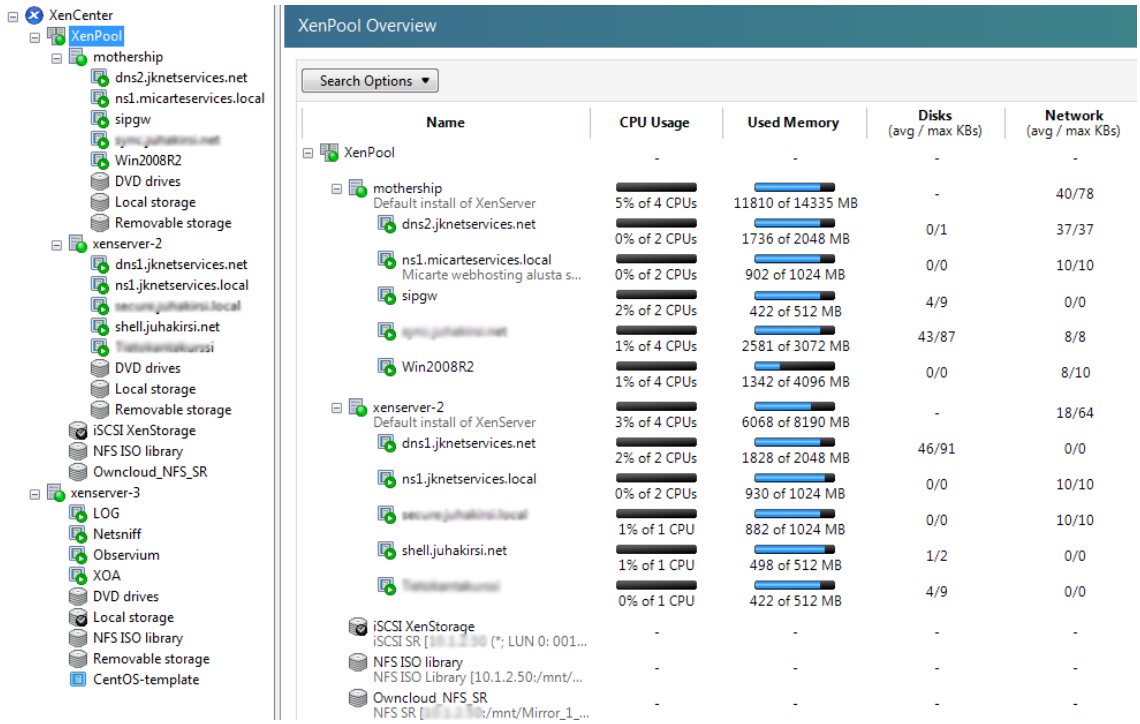
XCP-alustan käyttöönotto ei poikkea normaalin Linux-asennuksen kaavasta juuri millään tavalla. Asennuksen aikana valitaan levyosiot, joille se asennetaan, määritellään *root*-käyttäjälle salasana sekä määritellään hallintaverkolle verkkoasetukset. Suositeltu asennustapa on käyttää hallintaverkkoon omaa verkkokorttia tai verkkokortin porttia, tallennusjärjestelmälle omaansa sekä vierasjärjestelmien liikenteelle omaansa. XCP tai XenServer ei varsinaisesti tue käyttöjärjestelmän ohjelmallista RAID (Redundant Array of Independent Disks)-tilaa, joten jos käytössä ei ole laitteistoa, jossa olisi RAID-ohjainta, tulee tyytyä yhdelle kovalevylle asentamiseen. Tämä merkittävästi heikentää palvelimen vikasietoisuutta.

XCP-alustaa voidaan käyttää komentoriviltä *xe consolilla*- ja *xe*-alkuisilla komennoilla. Virtuaalikoneiden määrän kasvaessa voi olla hyvä käyttää järjestelmää komentorivipohjaisesti ja toimintoja skripteillä automatisoiden, mutta näin aluksi totesin kätevämmäksi käyttää Citrixin XenCenter-hallintakäyttöliittymää joka toimii XAPI-rajapinnalla (Xen Management API). Ohjelma on ilmainen, ja se on vapaasti ladattavissa XenServerin sivuilta. Uuden virtuaalikoneen luominen tapahtuu seuraamalla ohjattua luomisprosessia. Ensin valitaan käyttöjärjestelmän versio, joita on tarjolla useita eri versioita

Linuxista ja Microsoft Windowsista. Tämä määrittelee muotin, jonka perusteella uusi virtuaalikone luodaan. Seuraavaksi määritellään virtuaalikoneelle kuvaava nimi, joka voi olla mikä tahansa oman mielen mukainen nimitys ko. virtuaalikoneelle. Tämän jälkeen osoitetaan asennusmedia, joka voi olla isäntäkoneen paikallinen CD/DVD-asema (Digital Video Disc), levynkuvatiedosto tai verkkomedia. Pakollisia määrityksiä on vielä prosessoriytimien ja muistin määrä, kiintolevytiedoston koko sekä verkkokorttien asetukset.

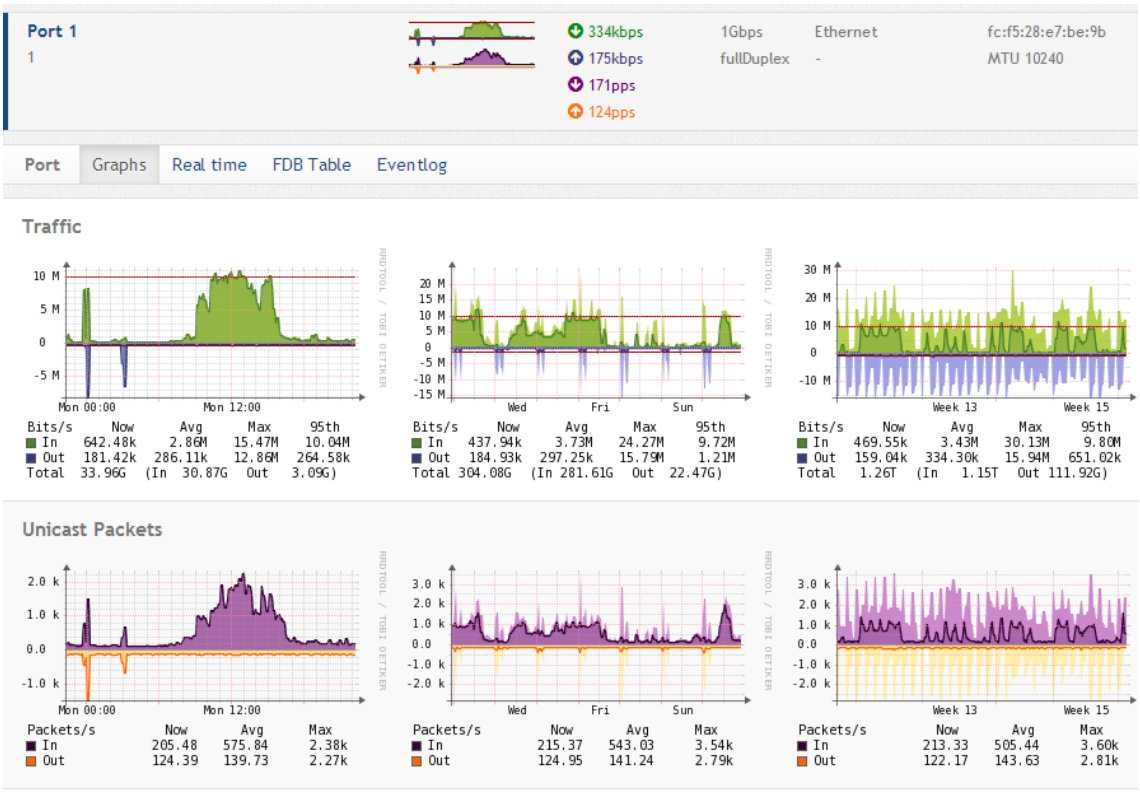
Kuvassa 12 näkyy XenCenter ohjelman hakemistopuu. Ylimpänä on XenPool-niminen klusteri, johon kuuluuvat isäntäpalvelimet mothership ja xenserver-2. Isäntäpalvelimien alla ovat virtuaalikoneet. Kuvassa näkyvistä virtuaalikoneista yksi on asiakkaalle toteutettu sisäinen järjestelmä, ja loput ovat omia sisäisiä ja ulkoisia palveluita.

Kuvassa näkyvä xenserver-3 ei kuulu xenpool-klusteriin. Kyseessä on erillinen isäntäpalvelin, jolla on ajossa erinäisiä raportointi ja monitorointisovelluksia. Näistä LOG-niminen toimii keskitettynä verkkolokipalvelimena, joka perustuu syslog-ng-nimiseen ohjelmistopakettiin. Tämän tarkoituksena on vastaanottaa ja arkistoida verkkolaitteiden ja tarvittaessa muiden palvelimien lokitiedot. Keskitetysti tallennettuja lokitietoja on mahdollisessa vikatilanteessa helpompi tutkia.



Kuva 12. Näkymä XenCenter hallintaohjelmaan.

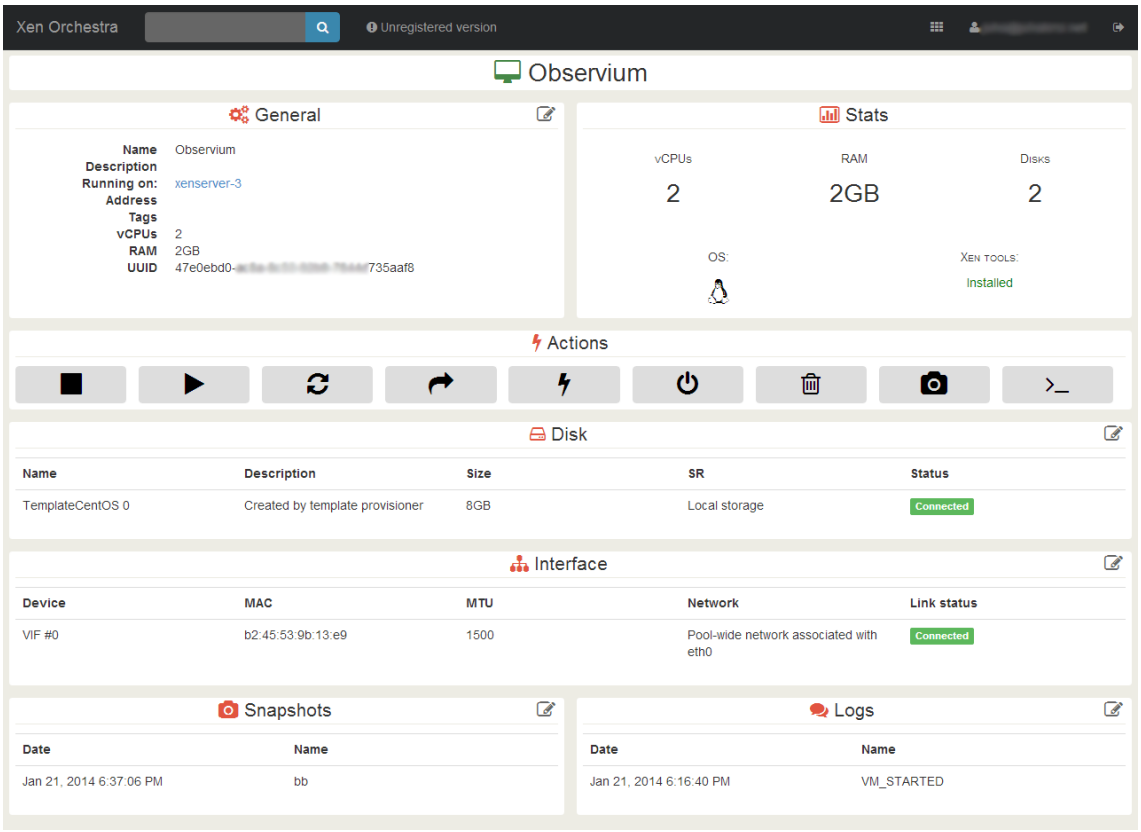
Observium-niminen virtuaalipalvelin pyörittää nimensä mukaista verkkovalvontasovellusta (Kuva 13). Järjestelmä perustuu SNMP-kyselyillä (Simple Network Management Protocol) tehtävään laitteiden jaksottaiseen kyselyyn. Netsniff-nimisen virtuaalikoneen tarkoitus on skannata määriteltyjä verkkoja ja hälyttää, mikäli se havaitsee uuden laitteen verkossa tai jos jo tunnettu laite häviää verkosta. Tämän taustalla toimii OverlookSoftin fing-ohjelma.



Kuva 13. Observium verkkovalvonta.

XOA-niminen (Xen Orchestra) virtuaalipalvelin on www-hallintaliittymä virtuaalikoneiden hallintaan, jos jostain syystä XenCenter ei olisi käytettävissä. XenCenter on tuettuna ainoastaan Windows käyttöjärjestelmälle, joten välillä tulee tilanne, jossa tarvitsee esimerkiksi käynnistää virtuaalikone uudelleen, mutta mukana on vain esimerkiksi Linux Mint-käyttöjärjestelmällä varustettu kannettava. XOA on tarjolla virtuaaliaplikaationa, eli tiedostona, joka sisältää virtuaalikoneen kiintolevytiedoston ja virtuaalikoneen määrittelevät asetukset. Se on myös saatavilla erillisinä paketteina käsin tehtävää asennusta varten. Itse tyydyin tässä vaiheessa valmisversioon, johtuen kokeiluluontoisesta käytöstä.

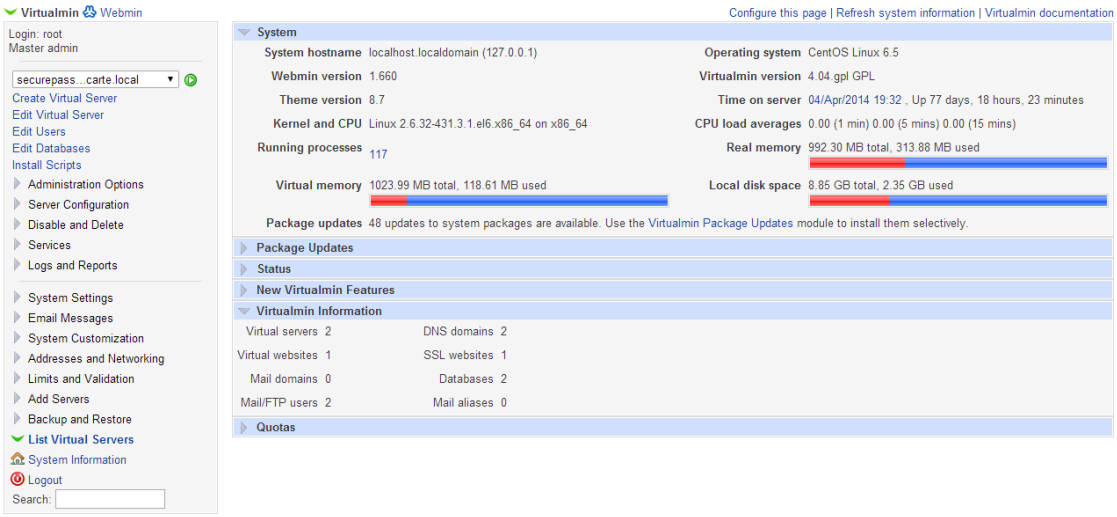
Kuvassa 14 näkyy XOA-järjestelmän näkymä yksittäisen virtuaalikoneen hallintasivusta.



Kuva 14. XOA www-hallintaliittymä.

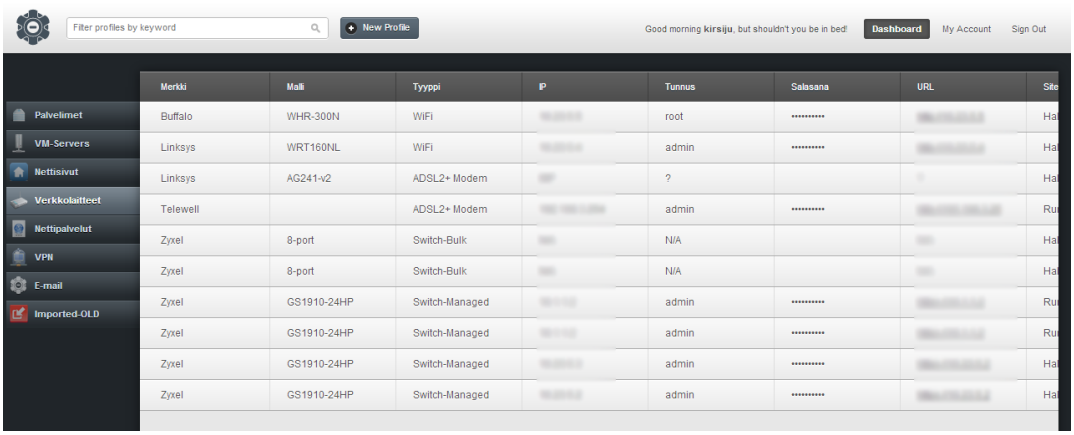
4.3 Asiakasjärjestelmän toteutus

Tmi M Designia varten asensin järjestelmään CentOS 6.5 Linux-käyttöjärjestelmän, jonka päälle asensin vielä Virtualmin GPL www-hostingalustan, jonka avulla on helppo toteuttaa yhdellä palvelimella, tässä tapauksessa virtuaalipalvelimella, usean eri www-pohjaisen sovelluksen tuottaminen. Virtuaalikone on asennusvaiheessa liitetty XenCenterin kautta määriteltyyn VLAN-verkkoon, joka on Tmi M Designia varten luotu. Virtuaalipalvelin on siis asiakkaan omassa yksityisessä VLAN-verkossa, jonne pääsy on palomuurilla rajattu.

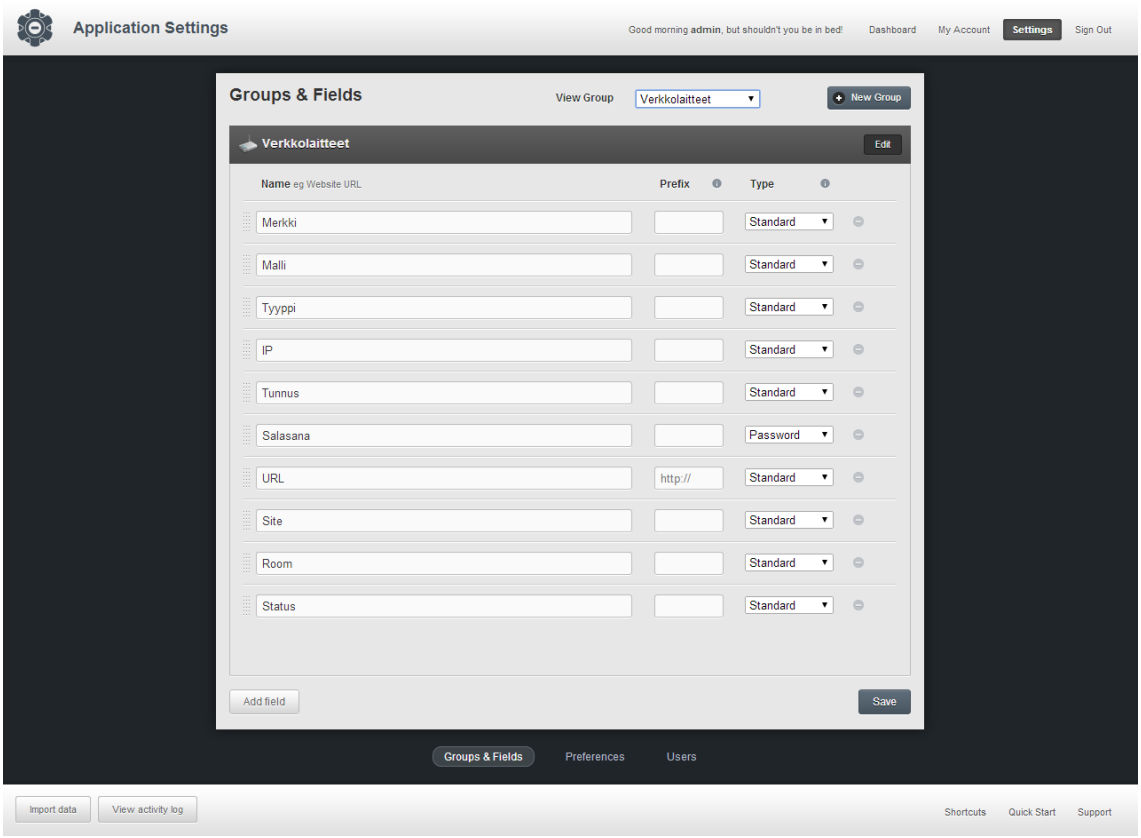


Kuva 15. Virtualmin GPL hosting-järjestelmän etusivu.

Kuvassa 15 näkyvälle Virtualmin alustalle määriteltiin käyttöön BIND (Berkeley Internet Name Domain)-nimipalvelin, MySQL-tietokantapalvelin sekä Apache-www-palvelin. Virtualmin alusta mahdollistaa palvelimen käytön nimipalvelimena asiakkaan verkolle sekä useiden uusien www-pohjaisten sovellusten käyttöönoton ilman, että niitä varten pitäisi luoda omia virtuaalipalvelimia. Näin isäntäpalvelimien resurssit eivät kulu turhaan jokaiselle yksittäiselle sovellukselle. Lisäksi Virtualmin mahdollistaa yksityiskohtaisempien varmuuskopioiden määrittelyn, verrattuna XenServerin kautta tehtävään virtuaalikoneen varmuuskopiomiseen. Alkuperäistä toimeksiantoa varten ensimmäiseen www-instanssiin asennettiin SimpleSafe-salasanojen hallintajärjestelmä. Kuva 16 näyttää, miltä salasanojen hallintajärjestelmä näyttää. Salasanakenttien sisältö on suojattu, jotta ne eivät olisi näkyvillä heti kun sivu avautuu. Viemällä hiiren salasanan päälle saa salasanan näkyviin ja tarvittaessa kopioitua leikepöydälle painikkeesta.



Kuva 16. SimpleSafe salasanojen hallintajärjestelmä.



Kuva 17. SimpleSafe-ohjelman asetukset.

Kuvassa 17 näkyvällä asetussivulta voidaan määritellä kenttien otsikot ja tietotyyppi. Salasana-tietotyyppiä käytettäessä kentän tieto ei näy suoraan sivua katseltaessa, eikä sitä tallenneta selkokielisenä tietokantaan. SimpleSafe ei julkisesti kerro tarkkoja salausmenetelmiään, mutta paljastaa, että siihen käytetään 256-bittistä salausmenetelmää ja jokaisella salasanalla on oma suola (salt) ja lisäksi tietokannalle on yksi pääsuola.

5 Tiedon varmistus

5.1 Tallennusjärjestelmät

Tiedon määrä on ollut viime vuosikymmeninä räjähdysmäisessä kasvussa, ja se on kasvattanut organisaatioiden tarvetta järkeistää tiedontallennusjärjestelmiään. Keskitetty tiedontallennus on nykypäivänä ehdoton vaatimus tiedonhallinnan ja turvaamisen kannalta. Tallennusjärjestelmien virtualisoinnilla tarkoitetaan loogisen tallennuslaitteen abstrahointia fyysisestä tallennuslaitteesta. Tallennusjärjestelmävirtualisointia voidaan tehdä laitetasolla tai verkkotasolla. Tämä mahdollistaa eri laitevalmistajien levyjärjes-

telmien levittämisen ympäri verkkoa ja kokoamisen yhteen tallennusjärjestelmävarantoon. Näin useita levyjärjestelmiä voidaan hallita keskitetysti. Virtualisoidut tallennusjärjestelmät tarjoavat paremman joustavuuden, yksinkertaisemman hallinnan sekä paremman suorituskyvyn ja tallennustilan käytön verrattuna perinteisiin paikallisiin levyjärjestelmiin.

Näiden ominaisuuksien käyttöön on kaksi pääasiallista järjestelmää; NAS (Network Attached Storage) ja SAN (Storage Area Network). Verkon kautta jaetun tallennusjärjestelmän käyttö on yksi vaatimuksista, jotta organisaatio voi hyödyntää palvelinvirtualisoinnin edistyneitä ominaisuuksia, kuten käynnissä olevan virtuaalikoneen migraatio isäntäpalvelimelta toiselle, varman saavutettavuuden palvelut (HA, High Availability), vikasietoisuus ja katastrofitilanteesta toipuminen [11, s. 16-17.]

Verkkoon liitetty tallennusjärjestelmä

Verkkoon liitetty tallennusjärjestelmä on tallennuslaite, joka on sijoitettu verkkoon, ja se tarjoaa palvelimille tallennustilaa. Se sallii useiden eri käyttäjien, kuten työasemien ja palvelimien, jakaa tiedostoja lähiverkossa. Verkkoon liitetyt tallennusjärjestelmät käyttävät tiedostojako protokolia, kuten NFS (Network File System) tai CIFS (Common Internet File System), jolloin on selvää, että tiedosto on verkossa ja kone pyytää tiedostoa, eikä esimerkiksi levylohkoa. Tällä tavalla tallennettu tieto on helposti hallittavissa yhdestä paikaista ja se on helpommin varmuuskopioitavissa. Koska verkkoon liitetty tallennusjärjestelmä on IP-pohjainen, se on helppo ottaa käyttöön ja hallita käyttäen nykyistä verkkoinfrastruktuuria [11, s. 17.]

Tallennusjärjestelmäverkko

Tallennusjärjestelmäverkko on laite, johon palvelimilla on pääsy niin, että laitteet vaikuttavat olevan paikallisesti kytkettyinä käyttöjärjestelmään. Tyypillisesti tällaisella laitteella on oma verkkonsa, johon tallennusjärjestelmät ovat kytkettyinä, eikä niihin tyypillisesti ole pääsyä tavallisilta laitteilta normaalin lähiverkon kautta. Tallennusjärjestelmäverkkolaite ei itsessään tarjoa tiedostotason palveluita, vaan ainoastaan lohkotason operaatioita. Useimmat tallennusjärjestelmäverkkolaitteet käyttävät kuituoptista verkkoa (Fibre Channel Connectivity), joka on erityisesti tallennusjärjestelmien kommunikointiin kehitetty verkkotekniikka, tai sitten iSCSI:a (Internet Small Computer System Interface), joka on IP-pohjainen verkkostandardi tallennusjärjestelmien yhdistämiseen [11, s. 18.]

5.2 Oma toteutukseni

Tallennusjärjestelmänä käytössä on palvelinlaitteistoon asennettu FreeNAS-käyttöjärjestelmä, joka on BSD-pohjainen avoimen lähdekoodin tuote. Asennettuna on kaksi 1,5 TB:n kiintolevyä *zMirror*issa, joka on ZFS (*Zettabyte File System*)-tiedostojärjestelmän RAID1-tilaa vastaava ohjelmistopohjainen peilaava tila. Peilatut levyt on jaettu tarpeen mukaan eri käyttöön esimerkiksi virtuaalikoneiden NFS- ja CIFS-jakoja, sekä iSCSI-osioita varten. FreeNAS kykenee tarjoamaan hyvän valikoiman NAS ja SAN järjestelmien ominaisuuksista. Valitsin peilaavan tilan johtuen levyjen määrästä. Peilaavassa tilassa ei tule suorituskykyhäviötä eikä hyötyä, mutta tieto on kahdennettua. Mikäli levyjä olisi enemmän, olisin valinnut RAID 0+1-tilan sen tuoman lisäsuorituskyvyn vuoksi. Neljällä levyllä teoreettinen nopeusetu valintaan verrattuna olisi kaksinkertainen lukunopeus ja kaksinkertainen kirjoitusnopeus.

Varmuuskopiointi

Ympäristön varmuuskopiointi on toteutettu kolmella tasolla. Ensimmäinen taso on yksittäisen virtuaalikoneen varmuuskopiointi, johon hyödynnetään XenCenterin VM Protection Policy -ominaisuutta. Palvelimille määritellään aikataulu, milloin niistä otetaan näköiskuva ja kuinka usein se tallennetaan ulkoiselle levylle. Tätä ei Tmi M Designin tapauksessa tehdä kuin kerran kuukaudessa, sillä alustana toimiva käyttöjärjestelmä ja Virtualmin alusta on melko stabiili muutoksien osalta.

Toinen taso on Virtualmin alustalta joka yö otettava varmuuskopio erilliselle levyjärjestelmälle jokaisesta www-instanssista. Varmuuskopio sisältää kaikki asetukset, tiedostot, käyttäjätunnukset ja tietokannat. Näitä kopioita säilytetään 60 päivää, jonka jälkeen ne poistetaan automaattisesti.

Kolmas taso on aamuyöllä tapahtuva tallennusjärjestelmän kahdennus varsinaisesta laitetilasta toiseen laitetilaan toisessa kaupungissa. Tällä varmistetaan tiedon säilyvyys mahdollisessa katastrofitilanteessa.

Palautus

Palautuspolkuja on erilaisia, ja niitä sovelletaan tilanteen ja tarpeen mukaan. Tällä hetkellä ”yhden klikkauksen” palautustoiminto toimii ensimmäisen ja toisen tason varmuuskopioille. Ensimmäisen tason varmuuskopioin palautus voi olla tarpeellinen yksittäisen isäntäpalvelimen vikaantuessa ja toisen tason varmuuskopion palautus tulee lähinnä kyseeseen yksittäisen virtuaalikoneen vikaantuessa tai käyttäjän virheestä johtuvassa vikatilanteessa.

Täydellisestä katastrofista palautumiseen tarvitaan korvaavaa laitteistoa, jolle asennetaan uusi XCP-virtualisointialusta sekä FreeNAS-levyjärjestelmä. FreeNAS-levyjärjestelmästä voidaan palauttaa viimeisin asetustiedosto, jolloin kaikkea ei tarvitse määritellä alusta saakka. Seuraavaksi on palautettava ensimmäisen tason varmuuskopiot eli yksittäisten virtuaalikoneiden tallennetut näköiskuvat. Nämä löytyvät kolmannen tason varmuuskopioista eli toissijaisesta palvelintilasta. Palautus tapahtuu käyttäen XenCenter-ohjelmistoa. Tämän jälkeen voidaan palauttaa viimeisin toisen tason varmuuskopio, jos sellainen on olemassa tai tarpeellinen. Se voidaan palauttaa virtuaalikoneen Virtualmin alustan www-hallintaliittymän kautta. Varmuuskopion palauttaminen osaa tarvittaessa vaihtaa palvelininstanssien IP-osoitteet Apache- ja BIND-ohjelmien konfiguraatiotiedostoihin.

6 Yhteenveto

Saavutetut tavoitteet ja kokonaisuus

Työn lähtökohdat huomioon ottaen työn voidaan katsoa onnistuneen, mutta kapasiteetti alkaa olla jo täynnä, eikä enempää asiakkaita toistaiseksi mahdu järjestelmään. Kokonaisuus kuitenkin toimii, kuten aluksi suunnittelin ja laajennusmahdollisuudet ovat olemassa.

Tmi M Designin tilaama kokonaisuus kattaa siis asiakaan koneelle asennettavan Viscosity VPN-ohjelmiston, jolla asiakas ottaa yhteyden Internet-yhteyden kautta palvelinsalin palomuuriin. Palomuurissa on määritelty asiakkaalle VPN-verkko, josta asiakasohjelma saa IP-osoitteen. Tälle verkolle on palomuurisäännöissä määritelty pääsy asiakkaan VLAN-verkkoon. Virtuaalialustalle asennettu virtuaalikone on kytketty kyseiseen verkkoon virtuaalijärjestelmän virtuaalikytkimellä. Virtuaalikoneelle asennettu

www-pohjainen salasananhallintajärjestelmä on siis käytettävissä mistä tahansa asiakkaan koneelta, josta sillä pääsee yhdistämään Internetiin. Yhteys kulkee Internetissä salattuna VPN-yhteyden sisällä, ja palvelinsalin verkoissa se on rajattuna omaan yksityiseen VLANiin.

Todetut ongelmat

Työn aikana on ongelmia koitunut lähinnä tallennusjärjestelmästä, sillä se toimii vanhimmalla palvelinlaitteistolla, josta on paristovarmennettu kirjoitusvälimuisti vanhentunut ja lakannut toimimasta. Sen lisäksi siinä käytettävät kiintolevyt ovat työasemakäyttöön suunnattuja virransäästöoptimoituja levyjä. Levyjärjestelmän suorituskyky on siis monilta osin riittämätön. Tämän voi todeta tekemällä virtuaalikoneella järjestelmän suorituskykymittauksia esimerkiksi dd-komennolla. Seuraava komento kirjoittaa tmp.out nimiseen tiedostoon nollia 1 GB:n verran. Toimenpiteen kestosta voi karkeasti päätellä levyjärjestelmän suorituskyvystä suuntaa.

```
dd if=/dev/zero of=tmp.out bs=1024 count=1000
```

Kehityskohteet

Kehityskohteina suunnitellulle toteutukselle näkisin palvelinlaitteiston päivittämisen niin, että jokaisessa palvelimessa on paristovarmennettu kirjoitusvälimuisti toiminnassa, sekä ylimääräisen verkkokortin lisääminen niin, että jokaisessa palvelimessa olisi vähintään neljä verkkoporttia käytettävissä verkkoliikenteelle. Näin voitaisiin eriyttää virtuaalikoneiden liikenne yhteen porttiin, hallintaverkko yhteen porttiin ja kaksi viimeistä porttia voitaisiin liittää yhdeksi loogiseksi portiksi tai pitää erillään ja kytkeä kahteen erilliseen tallennusjärjestelmäverkkoon. Tällä hetkellä käytössä on vain kaksi porttia isäntäkoneilla ja yksi portti tallennusjärjestelmässä. Isäntäkoneilla on eriytetty virtuaalikoneiden liikenne, ja toinen portti on jaettu hallintaliikenteelle ja tallennusjärjestelmäliikenteelle.

Tällä hetkellä kaikki liikenne kulkee yhden kytkimen kautta. Se sisältää julkisen verkon, hallintaverkon, tallennusjärjestelmän sekä jokainen yksityisen palvelinverkon liikenteen. Nämä tulisi eriyttää niin, että vähintään tallennusjärjestelmän liikenne saataisiin kulke-

maan omalle kytkimelle ja ideaalitilanteessa sekin olisi kahdennettu siten, että jokaisesta laitteesta kulkisi ethernet-kaapeli molempiin kytkimiin.

Suositeltavaa olisi myös tallennusjärjestelmän uusiminen joko täysiveriseksi tallennusjärjestelmälaitteeksi, tai vähintään uudempaan palvelinlaitteistoon perustuvaksi palvelimeksi, jossa olisi mahdollisuus kahdeksan 2,5”:n palvelinkiintolevyn liittämiseen.

Tämän jälkeen olisi mahdollista nostaa palvelukapasiteettiä useamman asiakkaan palvelemiseksi, lisäämällä isäntäpalvelimien muistia nykyisestä 8–14 GB:stä vähintään 32 GB:hen tai suurempaan.

Lähteet

1 What is VPN? - Part I. 2014. Verkkodokumentti. Cisco Systems <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/what_is_a_vpn.html>. Luettu 8.3.2014.

2 Network Security Protocols: IPsec vs. TLS/SSL vs SSH Part II. 2010. Verkkodokumentti. K2 Security Systems.<http://www.k2esec.com/secure-communications/network-security-protocols-ipsec-vs-tlsssl-vs-ssh-part-ii> . Luettu 31.3.2014.

3 Virtual Private Network. 2013. Verkkodokumentt. Khulna University Of Engineering & Technology.<http://www.slideshare.net/rushdishams/l4-vpn>. Luettu 31.3.2014.

4 Security Overview. 2014. Verkkodokumentti. OpenVPN Technologies Inc. <http://openvpn.net/index.php/open-source/documentation/security-overview.html>. Luettu 31.3.2014.

5 Is SSL a L4 or L7 VPN. 2011. Verkkodokumentti. The Cisco Learning Network. <https://learningnetwork.cisco.com/thread/25386>. Luettu 31.3.2014.

6 Getting Started. 2014. Verkkodokumentti. Electric Sheep Fencing LLC. <http://www.pfsense.org/about-pfsense/getting-started.html#overview>. Luettu 8.3.2014.

7 Features. 2014. Verkkodokumentti. Electric Sheep Fencing LLC. http://www.pfsense.org/about-pfsense/features.html#vpn>. Luettu 8.3.2014.

8 Virtuaalilähiverkko. 2013. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Virtuaalilähiverkko>. Päivitetty 10.3.2013. Luettu 6.3.2014.

9 VLAN-perusteet. 2014.Verkkodokumentti. Tallinna Ülikool. <http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html>. Luettu 6.3.2014.

10 VLAN-merkintä. 2014. Verkkodokumentti. Tallinna Ülikool. http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanmerkint.html>. Luettu 6.3.2014.

11 Golden Bernard, 2011. Virtualization For Dummies, 3rd HP Special edition. Wiley Publishing, Inc.

12 Rule David & Ditter Rogier, 2007. The Best Damn Server Virtualization Book Period. Syngress Publishing Inc.

13 Xen Overview. 2013. Verkkodokumentti. Xen Project. <http://wiki.xenproject.org/wiki/Xen_Overview#Xen_Paravirtualization_.28PV.29>. Luettu 4.4.2014.

14 IP Security (IPsec) and Internet Key Exchange (IKE) Document roadmap. 2011. Verkkodokumentti. Internet Engineering Task Force. <http://tools.ietf.org/html/rfc6071>. Luettu 13.4.2014.

15 Haavoittuvuustiedoite 076/2002. 2002. Verkkodokumentti. Viestintävirasto. <https://www.cert.fi/haavoittuvuudet/2002/varoitus-2002-76.html>. luettu 13.4.2014.

16 Remote Authentication Dial In User Service (RADIUS). 2000. Verkkodokumentti. Internet Engineering Task Force. <https://tools.ietf.org/html/rfc2865>. Luettu 14.4.2014.

17 Introduction to virtualization. 2012. Verkkodokumentti. OpenVZ Linux Containers. <http://openvz.org/Introduction_to_virtualization>. Luettu 14.4.2014.

18 Kernel Based Virtual Machine. 2013. Verkkodokumentti. Red Hat Emerging Technologies. <http://www.linux-kvm.org/page/Main_Page>. Luettu 14.4.2014.

19 Frequently Asked Questions. 2014. Verkkodokumentti. Humaan Pty Ltd. <https://www.simplesafe.net/faqs/>. Luettu 15.4.2014.

20 Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Verkkodokumentti. Internet Engineering Task Force. <http://www.ietf.org/rfc/rfc2459.txt>. Luettu 15.4.2014.

21 The Internet Key Exchange (IKE). 1998. Verkkodokumentti. Internet Engineering Task Force. <http://www.ietf.org/rfc/rfc2409.txt>. Luettu 15.4.2014.